METHOD AND SYSTEM FOR DYNAMICALLY DISTRIBUTING UPDATES IN A NETWORK

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to computer networking, and more particularly to a method and system for dynamically distributing updates in a network.

BACKGROUND OF THE INVENTION

Computer networks have become an increasingly important means for communicating public and private information between and within distributed locations. The Internet is one example of a public network commonly used for communicating public and private information. Internet web servers provide access to public information, such as news, business information, and government information, which the Internet makes readily available around the world. The Internet is also becoming a popular forum for business transactions, including securities transactions and sales of goods and services. A large number of people have come to depend upon reliable Internet access and secure communications on a day-by-day and even second-by-second basis. Like the Internet, private networks also have become common means for communicating important information. Private networks, such as company intranets, local area networks (LANs), and wide area networks (WANs) generally limit access on a user-by-user basis and communicate data over dedicated lines or by controlling access through passwords, encryption, or other security measures.

One danger to reliable and secure network communications is posed by hackers or other unauthorized users disrupting or interfering with network resources. The danger posed by unauthorized access to computer network resources can vary from simple embarrassment to substantial financial losses. For example, serious financial disruptions occur when hackers obtain financial account information or credit card information and use that information to misappropriate funds.

Typically, network administrators use various levels of security measures to protect the network against unauthorized use. Intrusion detection systems are commonly used to detect and identify unauthorized use of a computer

network before the network resources and information are substantially disrupted or violated. In general, intrusion detection systems look for specific patterns in network traffic, known as intrusion signatures to detect malicious activity. Conventional intrusion detection systems often use finite state machines, simple pattern matching, or specialized algorithms to identify intrusion signatures in network traffic. Detected intrusion signatures are reported to network administration.

A problem with conventional intrusion detection systems is that when a new vulnerability, or type of attack on the network, is discovered, a new intrusion signature must be generated and installed for each intrusion detection system. As a result, unless a network administrator frequently checks for new signatures developed by an intrusion detection provider and installs the new signatures for each sensor in his or her system, the system will remain vulnerable to the new types of attack. Because new types of attacks appear more frequently than network administrators typically check with an intrusion detection provider for new signatures, networks often remain vulnerable to new types of attacks even though new signatures are available to identify and prevent such attacks.

SUMMARY OF THE INVENTION

The present invention provides a method and system for dynamically distributing intrusion detection and other types of updates in a network that substantially eliminate or reduce disadvantages and problems associated with prior methods and systems. In particular, the present invention automatically downloads updates from a remote site in response to a timed event.

In accordance with one embodiment of the present invention, a first version of a program operating at a network site is updated by automatically downloading from a remote site any update for the program in response to an automated event. A downloaded update is installed to generate a second version of the program. The second version of the program is operated at the network site in place of the first version.

More particularly, in accordance with a particular embodiment of the present invention, the automated event is a timed event. In this embodiment, the first version of the program is aged and the timed event is the first version reaching a specified age. The specified age may be 24 hours or other suitable age. In other embodiments, the timed event may be a specified time such that any updates are automatically downloaded once a day, once a week, or at other suitable frequency.

After installation of a downloaded update, it may be determined whether the second version of the program is operating correctly. In response to incorrect operation of the second version, the first version of the program may be restored for operation at the network site. In response to correct operation of the second version, the downloaded update may be distributed to disparate network sites operating the first version of the program. There, the downloaded update may be installed to generate the second version of the program at the disparate network sites. The

second version of the program is operated in the place of the first version at the disparate network sites.

Technical advantages of the present invention include providing an improved method and system for distributing updates in a network. In particular, programs are automatically updated by downloading and distributing an update in response to an automated event, such as a timed event. As a result, systems with a common program separately running at several sites may update each site with no or minimal operator interaction. In addition, updates may be automatic or with minimal operator interaction rolled back at each site in a system in response to an upgrade problem.

Additional technical advantages of the present invention include providing an improved intrusion detection system. In particular, each intrusion detection sensor may automatically connect to a remote site and download new intrusion detection signatures. Each sensor may also distribute the new signatures to related sensors within a system. Accordingly, network vulnerability due to new types of attacks is reduced. In addition, an intrusion detection service provider may update all of its customers by simply providing new signatures on a website from which each customer's system will automatically connect to and download the new signatures in accordance with a specified frequency. Accordingly, the costs of providing intrusion detection services are reduced.

Other technical advantages will be readily apparent to one skilled in the art for the following figures, description, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like reference numerals represent like parts, in which:

FIGURE 1 is a block diagram illustrating a system for dynamically distributing intrusion detection signatures in accordance with one embodiment of the present invention;

FIGURE 2 is a flow diagram illustrating a computer method for dynamically distributing intrusion detection signatures in the network of FIGURE 1; and

FIGURE 3 is a flow diagram illustrating a computer method for recovering from a problematic update in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 is a block diagram illustrating a system 10 for dynamically distributing updates in a network. In this embodiment, new intrusion signatures are distributed to remote intrusion detection sensors. The sensors use the intrusion signatures to detect and report unauthorized entry. It will be understood that the present invention may be used to distribute other suitable types of updates to intrusion detection and other suitable types of applications within a network.

Referring to FIGURE 1, the system 10 includes a private network 12 and a public network 14. For the embodiment of FIGURE 1, the private network is an Intranet 20 and the public network is an Internet 22. It will be understood that the private and public networks 12 and 14 may be other suitable types of networks.

The Intranet 20 includes a network interconnecting a plurality of hosts 24. The network is a local area network (LAN), a wide area network (WAN), or other suitable type of link capable of communicating data between the hosts 24. For the local area network embodiment, the network may be an Ethernet.

The hosts 24 are each a computer such as a personal computer, file server, workstation, minicomputer, mainframe or any general purpose or other computer or device capable of communicating with other computers or devices over a network. The hosts 24 operating on the border between the Intranet 20 and Internet 22 each include an intrusion detection sensor 26 for detecting and reporting unauthorized entry. As used herein, each means each of at least a subset of the identified items.

The intrusion detection sensors 26 each include a common set of intrusion signatures 28. The intrusion signatures 28 comprise patterns of network activity that denote or indicate unauthorized access or other harmful

activity capable of damaging the host 24 or other aspect of the private network 12. Generally described, the intrusion detection sensors 26 detect such unauthorized access or attacks upon the host 24 by matching network traffic to the intrusion signatures 28.

The Internet 22 includes a sensor update server 30. The sensor update server 30 may be virtually any type of computer capable of storing intrusion updates 32 and communicating with other computers or devices over the Internet 22. The intrusion update 32 includes new intrusion signatures generated by an intrusion detection service provider in response to new types of attacks. The intrusion detection service provider generates the new signatures and provides them as the update 32 on a web page at the sensor update server 30 to allow customers to access the new signatures over the Internet 22. As described in more detail below, the update 32 is downloaded by customers over the Internet 22 and the new signatures added to the intrusion signatures 28 residing on the host 24. In this way, the intrusion detection sensors 26 are kept up-to-date and able to detect and report new types of network and/or host based attacks.

FIGURE 2 is a flow diagram illustrating a computer method for dynamically distributing intrusion detection updates over the Internet 22 or other suitable network. It will be understood that other types of updates for other types of applications may be similarly distributed over the Internet 22 or other suitable network without departing from the scope of the present invention.

Referring to FIGURE 2, the method begins at step 50 in which a specified event is received. The specified event may be an automated event or a user initiated event. The automated event may be any event generated by the sensor or other software or hardware in accordance with predefined instructions or logical set of such events. In one

embodiment, the automated event is a timed event that is directly or indirectly based upon the reaching or passing of a specified time. For this embodiment, the intrusion detection sensors 26 may automatically age the intrusion signatures 28 after each update to allow the intrusion detection sensors 26 to automatically determine when the intrusion signatures 28 may be in need of updating. In this embodiment, an update event is generated in response to the intrusion signatures 28 reaching a specified age. The age is twenty-four hours or other suitable time period that will allow the intrusion signatures 28 to be updated at a frequency that will minimize vulnerability of the private network 12 to new types of attacks. An event or action is in response to a specified event when the occurrence of the specified event directly or indirectly triggers, at least in part, the responding event or action. Thus, other events may also be necessary to trigger the responding event or action, or intervene between the specified event and the responding event or action. The update event may be other suitable types of timed events such as, for example, a specified or scheduled time of day, week, or the like.

In a particular embodiment, a user may select a number of sensors to be subordinate to a primary intrusion detection sensor or set of primary sensors. In this embodiment, only the primary sensors are responsible for generating the update event and only their intrusion signatures 28 are aged. Alternatively, each intrusion detection sensor 26 may independently age its own intrusion signatures 28 and generate the update event in response to its intrusion signatures 28 reaching the specified age. In this embodiment, no one intrusion section sensor 26 or limited set of sensors is solely relied upon to initiate updating.

Proceeding to step 52, the intrusion detection sensor 26 generating the update event automatically connects to the sensor update server 30 over the Internet 22. At decisional step 54, the intrusion detection sensor 26 automatically determines whether the sensor update server 30 includes an update 32 for the intrusion signatures 28. In one embodiment, the intrusion detection sensor 26 may compare a time stamp of its last update to that of a current file on the sensor update server 30. In this embodiment, the current file is an update 32 if the time stamp for the file is later than that for the last update for the intrusion detection sensor 26. If an update 32 is not available, then the current set of intrusion signatures 28 are up-to-date and the No branch of decisional step 54 leads to the end of the process. Accordingly, the intrusion signatures 28 are updated only when needed. However, if an update 32 is available on the sensor update server 30, the Yes branch of decision step 54 leads to step 56.

At step 56, the intrusion detection sensor 26 automatically downloads the update 32. Preferably, the update 32 is downloaded in an encrypted format to prevent tampering and decrypted at the host 24. In addition, the update 32 may be protected by VPN, sequence numbering, other suitable form of secure communication, or a combination of forms. Next, at decisional step 58, the intrusion detection sensor 26 automatically authenticates the update 32. In one embodiment, the update 32 is authenticated by ensuring that the update is for the existing set of intrusion signatures 28. If the update 32 is not authentic, then it should not be installed and the No branch of decisional step 58 leads to the end of the process. Accordingly, an update 32 that cannot be authenticated is not installed. However, if the update 32

is authentic, the Yes branch of decisional step 58 leads to step 60.

At step 60, the intrusion detection sensor 26 automatically installs the update 32 to add the new signatures to the preexisting intrusion signatures 28. Next, at decisional step 62, the intrusion detection sensor 26 automatically determines if it is operating correctly with the installed update by comparing its operation to specified parameters, limits, and the like. If the intrusion detection sensor 26 is not operating correctly, then the No branch of decisional step 62 leads to step 64 where recovery processing is automatically initiated and the update 32 is uninstalled. Accordingly, the intrusion detection sensor 26 is returned to its previous state and the private network 12 is not left vulnerable by an incorrectly operating intrusion detection sensor 26. However, if the update intrusion sensor 26 is operating correctly, the Yes branch of decisional step 62 leads to step 66.

At step 66, the intrusion detection sensor 26 automatically broadcasts an update message over the Intranet 20. The update message informs the other intrusion detection sensors 26 of the availability of the update 32. Next, at step 68, the update 32 is automatically transmitted to the intrusion detection sensors 26 that responded to the update message. In one embodiment, the update message identifies the update and intrusion detection sensors 26 not having that update respond to request the update 32. The update 32 may be transmitted over the Intranet 20 in an encrypted format and a secure form and decrypted by each of the second stage intrusion detection sensors 26 as previously described for the first stage intrusion detection sensor 26 that originally received the update 32. If a sensor hierarchy is used, relationships between primary and secondary

sensors may be predefined with the primary sensors each sending updates 32 to their respective secondary sensors. In addition, the relationship may be recursive with secondary sensors having their own children.

Proceeding to decisional step 70, each of the second stage intrusion detection sensors 26 authenticates the update 32 as previously described in connection with the first stage intrusion detection sensor 26. If the update 32 cannot be authenticated by a second stage intrusion detection sensor 26, the No branch of decisional step 70 returns to step 68 for that second stage intrusion detection sensor 26 where the update 32 is retransmitted to the intrusion detection sensor 26. Alternatively, or in response to several unsuccessful attempts to transmit an authentic update 32 to a second stage, the No branch of decisional step 70 may lead to the end of the process where the update 32 is not installed for that intrusion detection sensor 26. After an authentic update 32 is received by a second stage intrusion detection sensor 26, the Yes branch of decisional step 70 leads to step 72.

At step 72, the update 32 is automatically installed for each of the second stage intrusion detection sensors 26 receiving an authentic update 32 to generate an updated set of intrusion signatures 28. Accordingly, all intrusion detection sensors 26 in the private network 12 are automatically updated to protect all avenues of access to the private network 12 from the new types of attacks.

Proceeding to decisional step 74, each of the second stage intrusion detection sensors 26 determine if they are operating correctly with the installed update 32. If a second stage intrusion detection sensor 26 is not operating correctly, the No branch of decisional step 74 leads to step 76. At step 76, recovery process is initiated for that intrusion detection sensor 26 and the update 32 is uninstalled. In this way, it is ensured that each of the

second stage intrusion detection sensors 26 will remain in operating condition. For each second stage intrusion detection sensor 26 operating correctly with the installed update 32, the Yes branch of decisional step 74 leads to the end of the process. Accordingly, all intrusion detection sensors 26 for the private network 12 have been automatically updated. Because user interaction is not required, the intrusion detection sensors 26 may be frequently and efficiently updated to ensure that the private network 12 is not vulnerable to new types of attacks.

It will be understood that the intrusion sensors 26 may be otherwise suitably updated without departing from the scope of the present invention. For example, although the method was described with the intrusion detection sensor 26 performing the specified actions, it will be understood that another application in or remotely from the hosts 24 may carry out the updating functionality identified for the intrusion detection sensor 26.

FIGURE 3 illustrates a computer method for recovery processing in accordance with one embodiment of the present invention. Referring to FIGURE 3, the method begins at step 90 in which a recovery event is received. The recovery event may be initiated by an intrusion detection sensor 26 in response to incorrect operation of the intrusion detection sensor 26. The recovery event may also be independently initiated by an operator to uninstall the update 32.

Proceeding to step 92, the update 32 is uninstalled from a first intrusion detection sensor 26. The first intrusion detection sensor 26 may be the first sensor 26 on which the update 32 was initially installed or another intrusion detection sensor 26 detecting incorrect operations or receiving a user command to initiate recovery

processing. Uninstalling the update 32 returns the first intrusion detection sensor 26 to its previous state.

Next, at step 94, the first intrusion detection sensor 26 transmits a recovery message to the remaining intrusion detection sensors 26 in the private network 12 on which the update 32 was installed. Next, at step 96, each of the remaining intrusion detection sensors 26 uninstalls the update 32 in response to the recovery message. Accordingly, each intrusion detection sensor 26 in the private network 12 is returned to its previous state in response to a single recovery event. In this way, integrity of the private network 12 and the intrusion detection system for the private network 12 is maintained with each of the intrusion detection sensors 26 in a same state. Step 96 leads to the end of the process by which each of the intrusion detection sensors 26 have been returned to a same recovery state.

Although the present invention has been described with several embodiments, various changes and modifications may be suggested to one skilled in the art. It is intended that the present invention encompass such changes and modifications as fall within the scope of the appended claims.